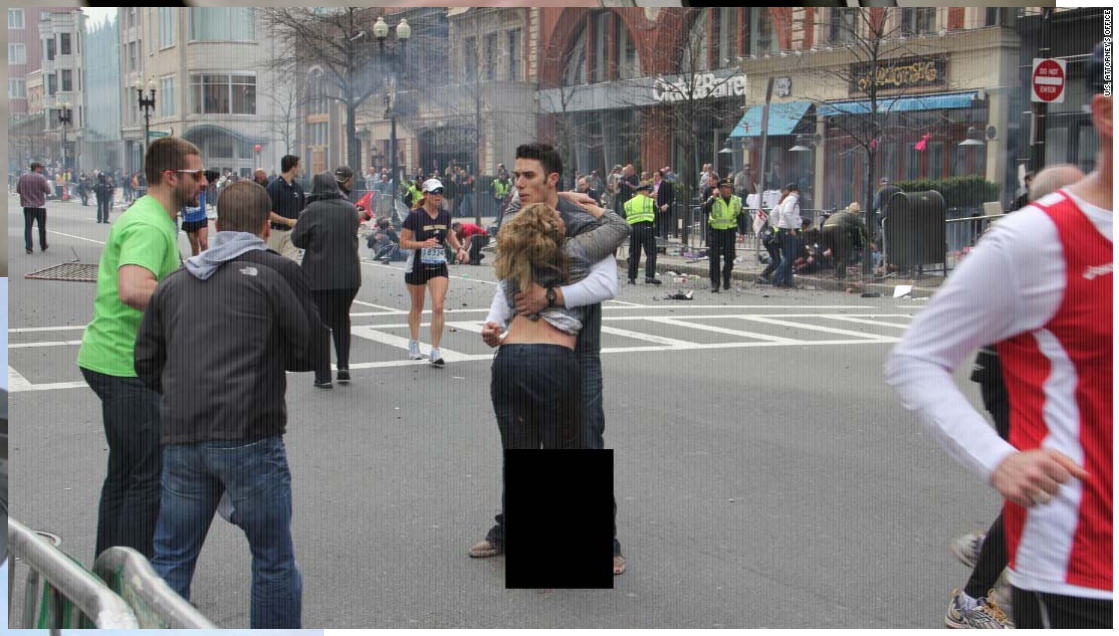
UNISYS | Securing Your Tomorrow™

Privacy and Surveillance-Based Biometrics: Pushing Boundaries

Surveillance and Informed Consent

- Approximately 30,000 – 40,000 fixed surveillance cameras in Sydney
  Sydney Morning Herald ***2007***
- Sydney trains awards contract in 2016 for 11,400 CCTV cameras



What's next?

Surveillance and Biometrics

Age, Gender, Ethnicity

- Facial recognition

Usage:

- Customisation of user interface
- Statistics analysis
- Grouping/targeting

Anonymous Monitoring

- Face/voice recognition, pattern recognition, gait recognition

Usage:

- Track movement
- Monitor activities
- Determine relationships
- Build gallery of unknown individuals

Identification

- Face, voice, iris recognition
- Link anonymous person to known identity (e.g., credit card)

Usage:

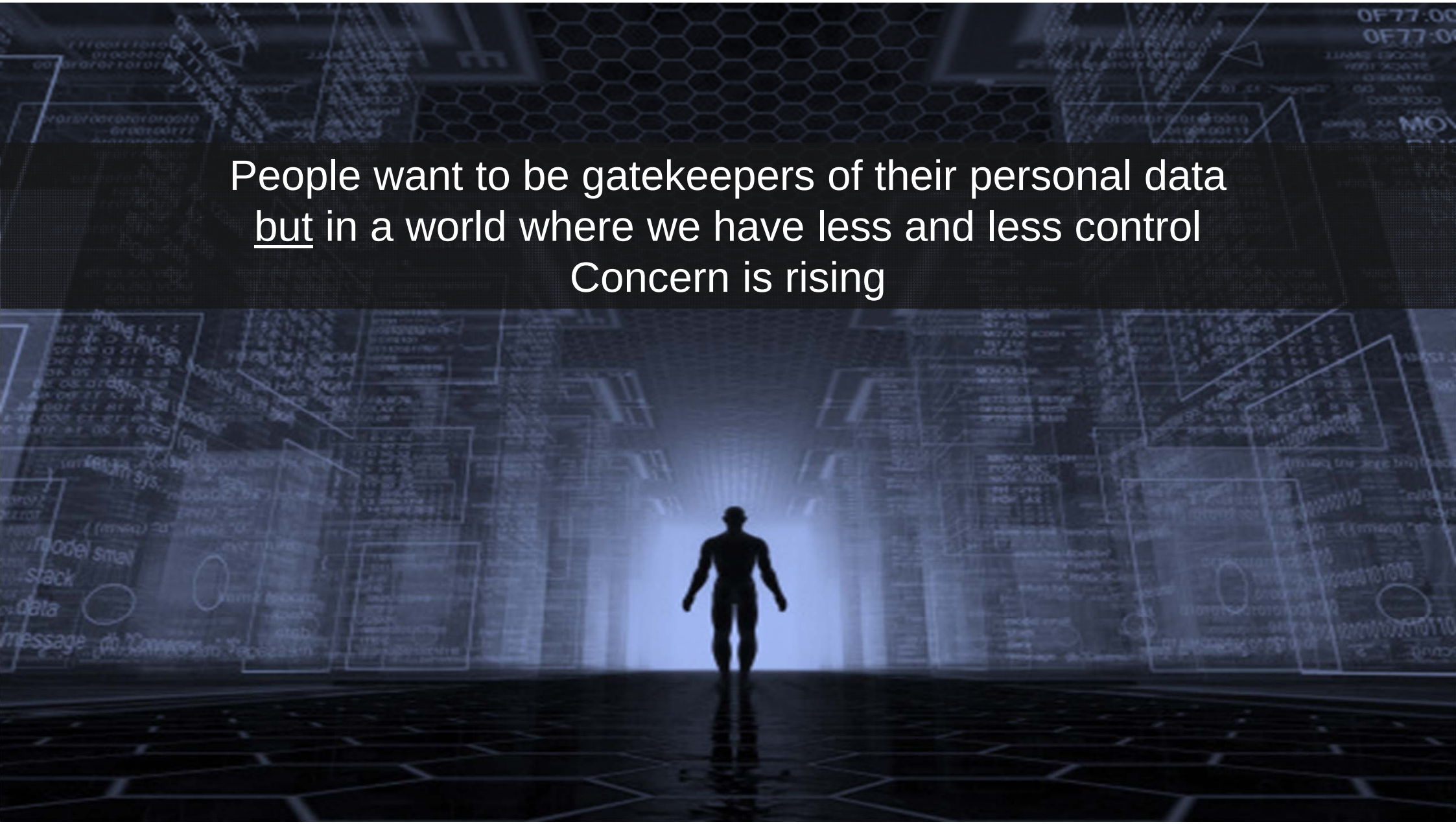
- Identify persons of interest (watch list)
- Targeted treatment

Biometrics and Continuous Authentication

Keystroke identification

Gesture identification

Voice identification


People want to be gatekeepers of their personal data
but in a world where we have less and less control
Concern is rising

Is it just a matter of weighing the pros and cons?

Benefits

- Enhanced safety and security
- Customised service
- Ease of doing business

Dangers

- Function creep abuse
- Breaches / identity theft
- Erroneous identification

Or should we let the majority decide?

Unisys Security Index

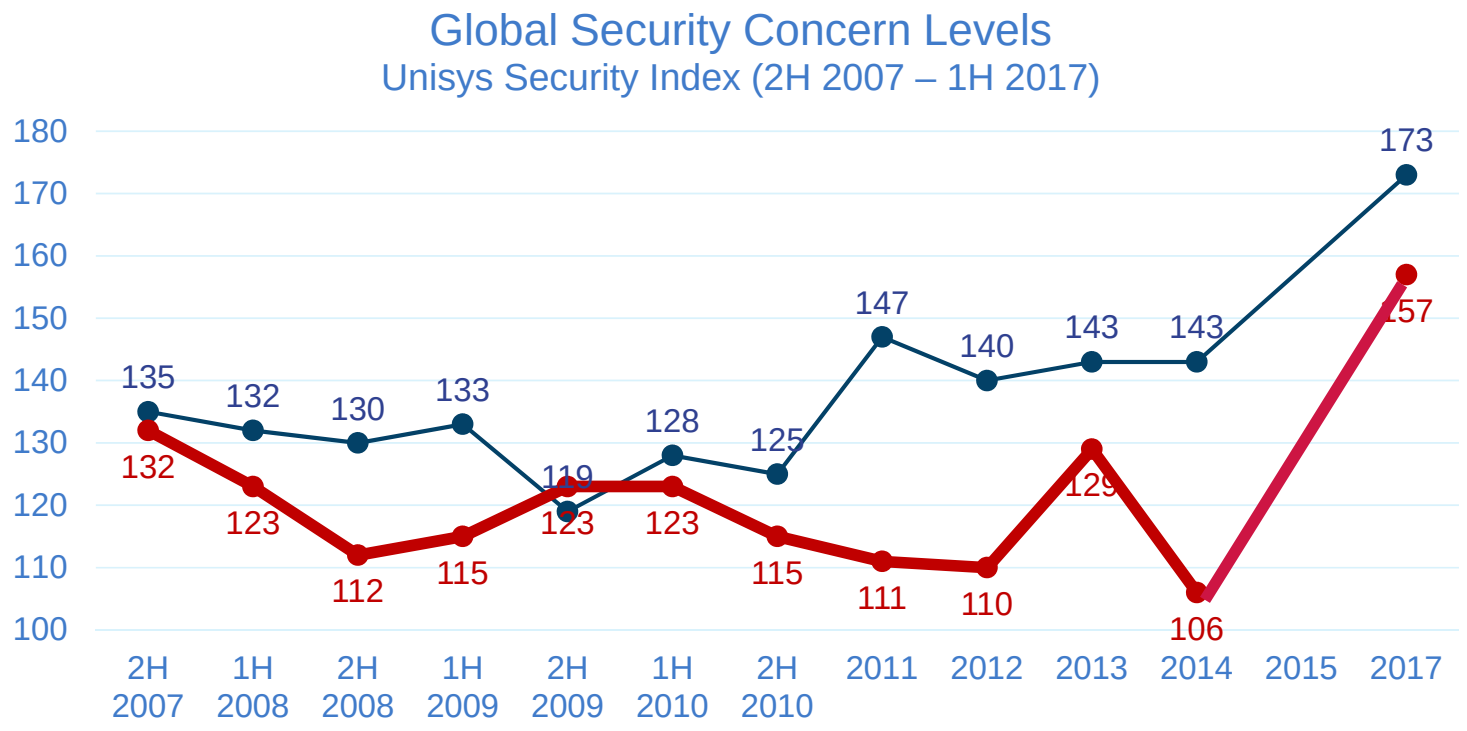
NATIONAL SECURITY	NATIONAL SECURITY	Your Country's national security in relation to war or terrorism
	DISASTER/ EPIDEMIC	A serious natural disaster occurring in Your Country
FINANCIAL SECURITY	BANKCARD FRAUD	Other people obtaining and using your credit or debit card details
	FINANCIAL OBLIGATIONS	Your ability to meet your essential financial obligations
INTERNET SECURITY	VIRUSES/ HACKING	Computer and Internet security in relation to viruses, unsolicited emails or hacking
	ONLINE TRANSACTIONS	The security of shopping or banking online
PERSONAL SECURITY	IDENTITY THEFT	Unauthorized access to, or misuse of your personal information
	PERSONAL SAFETY	Your overall personal safety over the next 6 months

Poll consumer concerns across:

- 4 areas of security via
- 8 questions
- Calculate score 0-300

Unisys Security Index

Australian Security Concerns are High and Rising



+30 Global

+51 Australia

UNISYS | Securing Your Tomorrow™

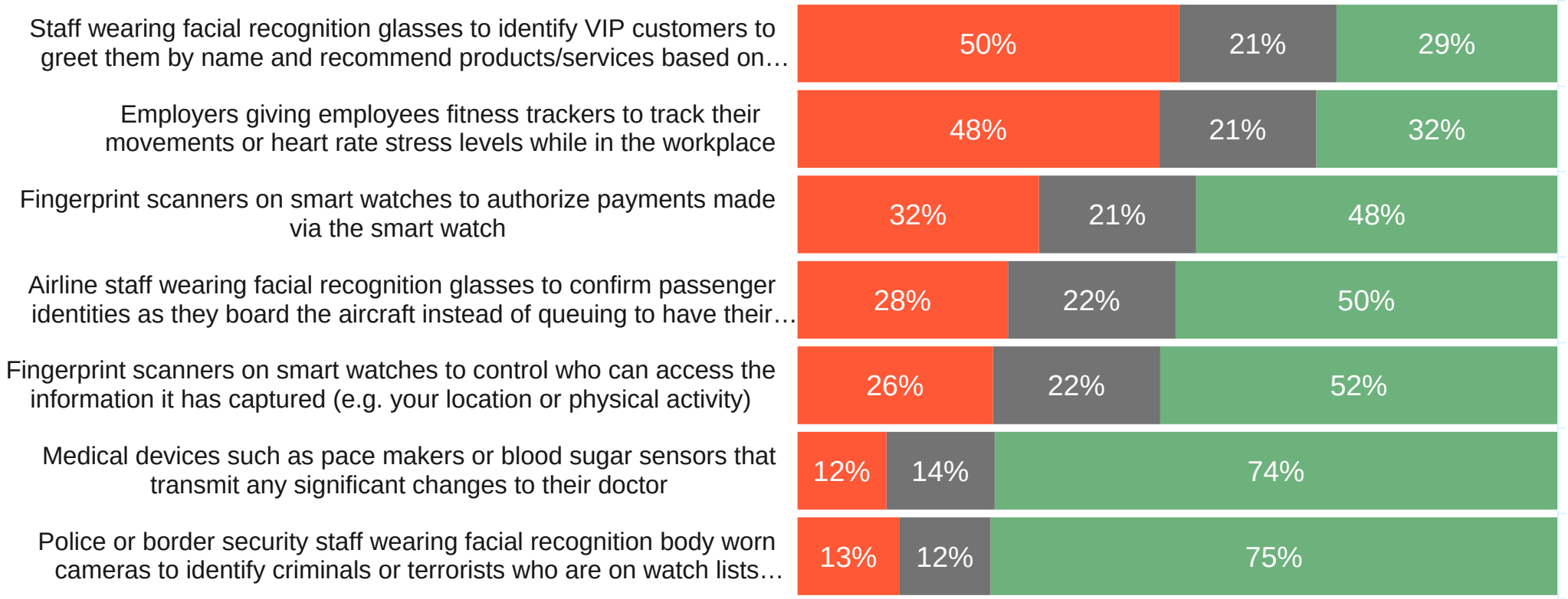
Top Security Concerns - Australia

Data privacy issues remain the top security concern for Australians

UNISYS | Securing Your Tomorrow™

How do Australians feel about biometrics?

Please say whether you support or don't support the following scenarios



Unisys Security Index – Australia (2017)

UNISYS | Securing Your Tomorrow™

Should a vocal minority decide for the majority?

Do the desires of the few outweigh the desires of the many?

How to deal with risks?

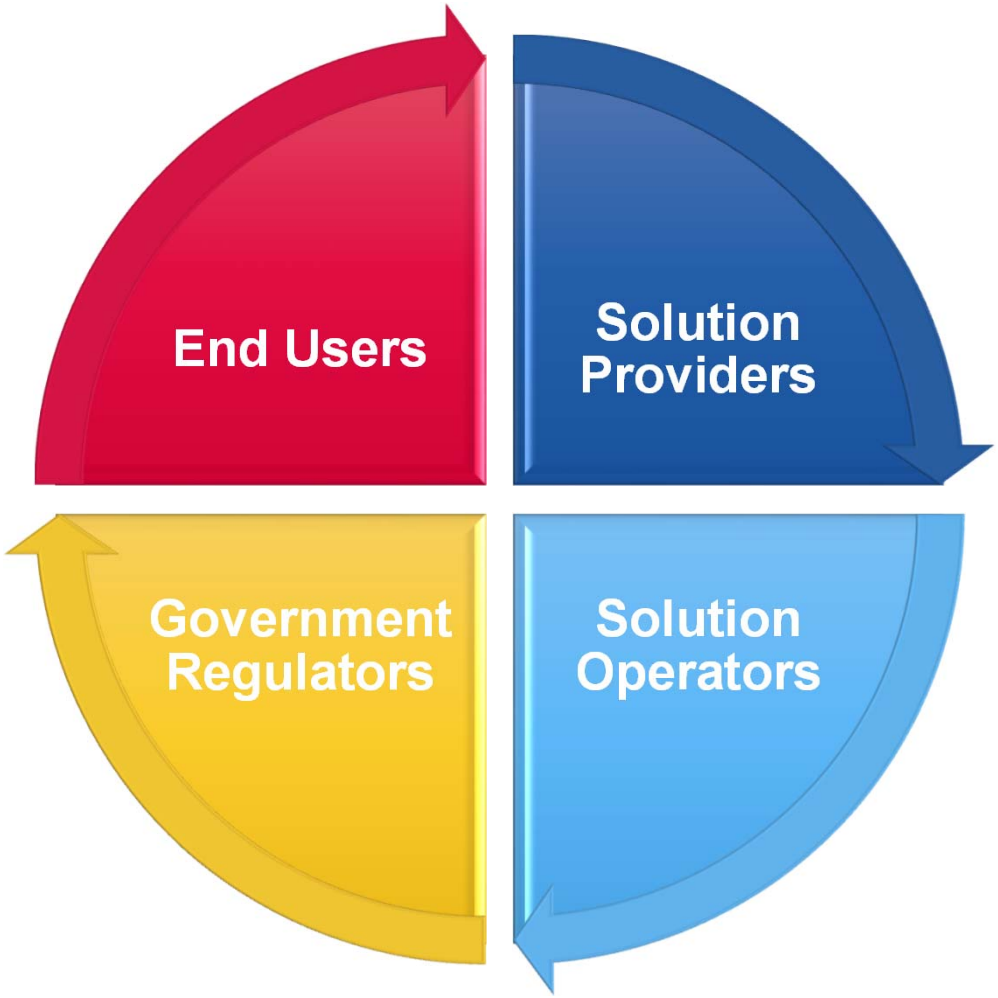
Accept

Avoid

Reduce

Transfer

Risk Transfer



Risk Transfer / Share

Share risk with End Users:

- Informed Consent
- Opt-in / Opt-out
- Recommended/enforced security measures

Share risk with Solution Providers:

- Shared Liability
- Mandatory standards for duty of care
- Penalties for non-compliance

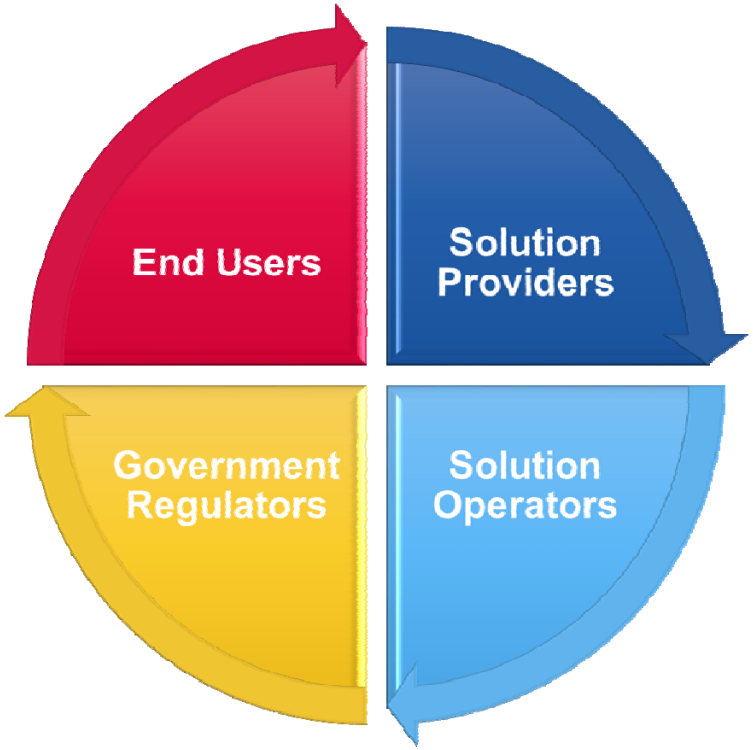
Role of Biometrics Institute – Privacy Guidelines

Purpose:

- ❖ Guide all stakeholders
- ❖ Assure the public
- ❖ Guide for all countries and jurisdictions

1. Respect for Individuals/data subject privacy
2. Proportionality
3. Informed Consent
4. Truth and Accuracy in Business Operations
5. Protection of Biometric Data Collected
6. Complaints and Enquiries
7. Purpose
8. Non-discrimination
9. Accountability
10. Sharing of Biometric Data
11. Provision of Advance Warnings of Surveillance
12. Transmission of Biometric Data beyond National Boundaries
13. Employee Biometric Data must be Protected
14. Limit the Extent of Personal Data Exchanged and Retained
15. Maintain a Strong Privacy Environment
16. Individual Participation / Subject Access

Risk Reduction



- ✓ **Compliance with applicable laws and regulations**
- ✓ **Compliance with Biometrics Institute Privacy Guidelines**
- ✓ **Go the extra mile to protect biometric data against unauthorised access**
  - Authorised Users vs Zero Trust Model
  - Assume internal environment is hostile
  - Assume external hackers will get in
  - Assume operators and end users are the weak link
  - Implement strategies to deter and contain breaches

Key Take-Aways…

The convergence of surveillance and identification is happening faster and broader than can be managed by privacy legislation – personal privacy is at grave risk!

When considering new biometric applications, avoid the extremes of risk intolerance and risk ignorance – focus first on risk sharing and risk management

Ensure that biometric solutions respect and protect the privacy of the individual using technology designed to protect the most sensitive data against the most challenging threats

Want to know more?

Download the Unisys Security Index Australia and global reports
www.unisys.com/unisys-security-index/australia

For information on Unisys security solutions

visit
www.unisys.com/security

email
Info-Security@unisys.com

Join the conversation
#Unisys #SecurityIndex

Biometrics Institute Privacy Guidelines
http://www.biometricsinstitute.org/pages/privacy-charter.html

UNISYS | Securing Your Tomorrow™

Thank You

UNISYS | Securing Your Tomorrow™